Litchko & Associates, Inc.

Secure Business-based Solutions^{tm}

Countering the Insider Threat

The right way and the wrong way.

September 25, 2003

Jim Litchko
301-661-3984
jim@litchko.com

Background and Experience

100 information system security assessments

30 years attacking and protecting systems

20 years Navy SIGINT and INFOSEC

15 years security instructor

10 years commercial

5 years at NSA

Opinions

RISK

Questions:

- **What is It?**
- **Who is It?**
  - –
  - –
  - –
  - –
  - –
  - –
- **How do I do about It?**

Confidentiality

- Ensuring that the information is only available to authorized entities.
- Other words used are: “Secrecy”, “Privacy”, . . .

Integrity

- Ensuring that the information has not been changed.
- Other words used are: “Accuracy”, “Authentic”, “Correct”, ...

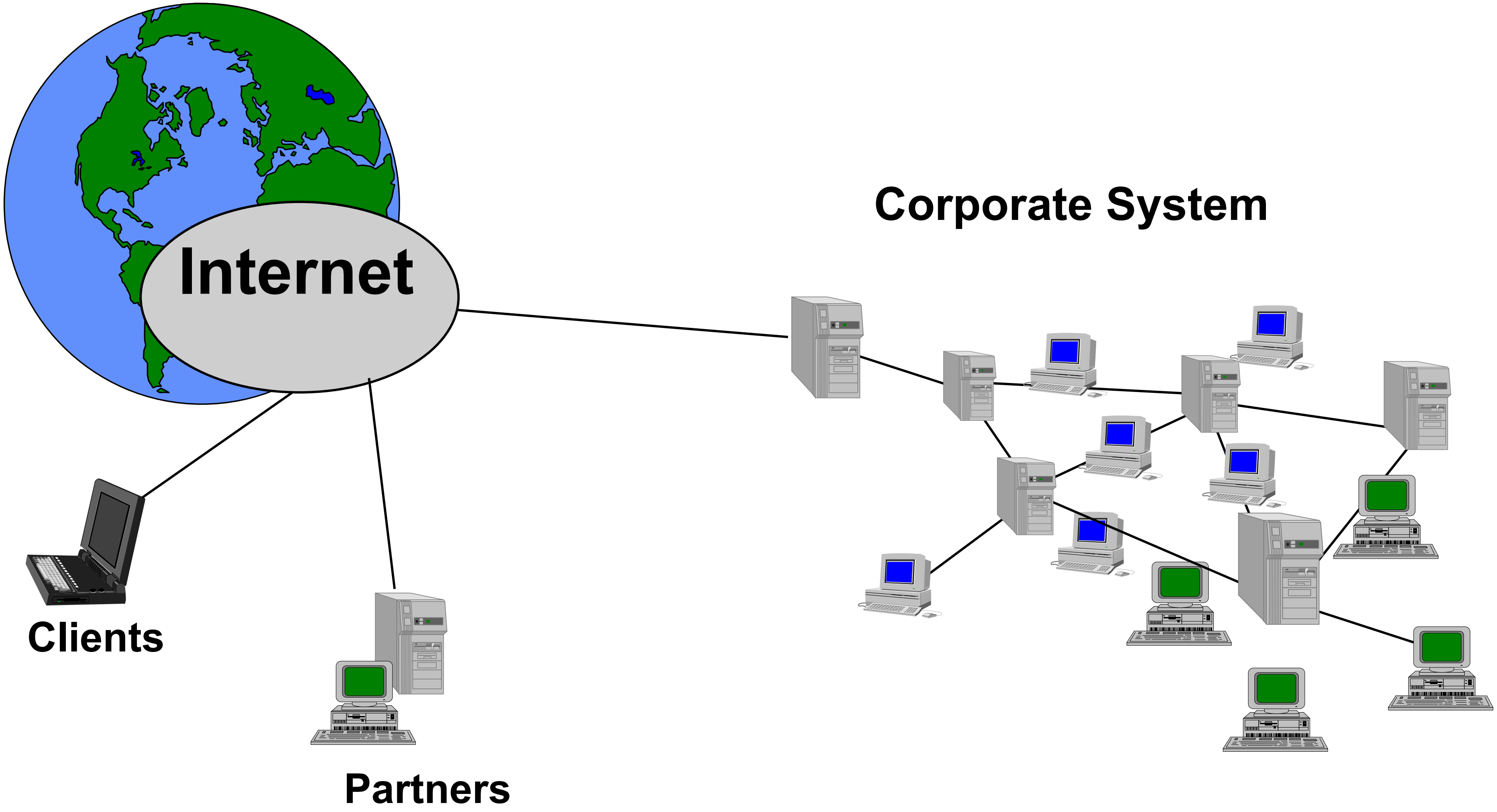
Authentication

- Proving that a user or system is what they claim to be.
- Other words are: “Identification”, “Authorized”, “One of the good people”. .

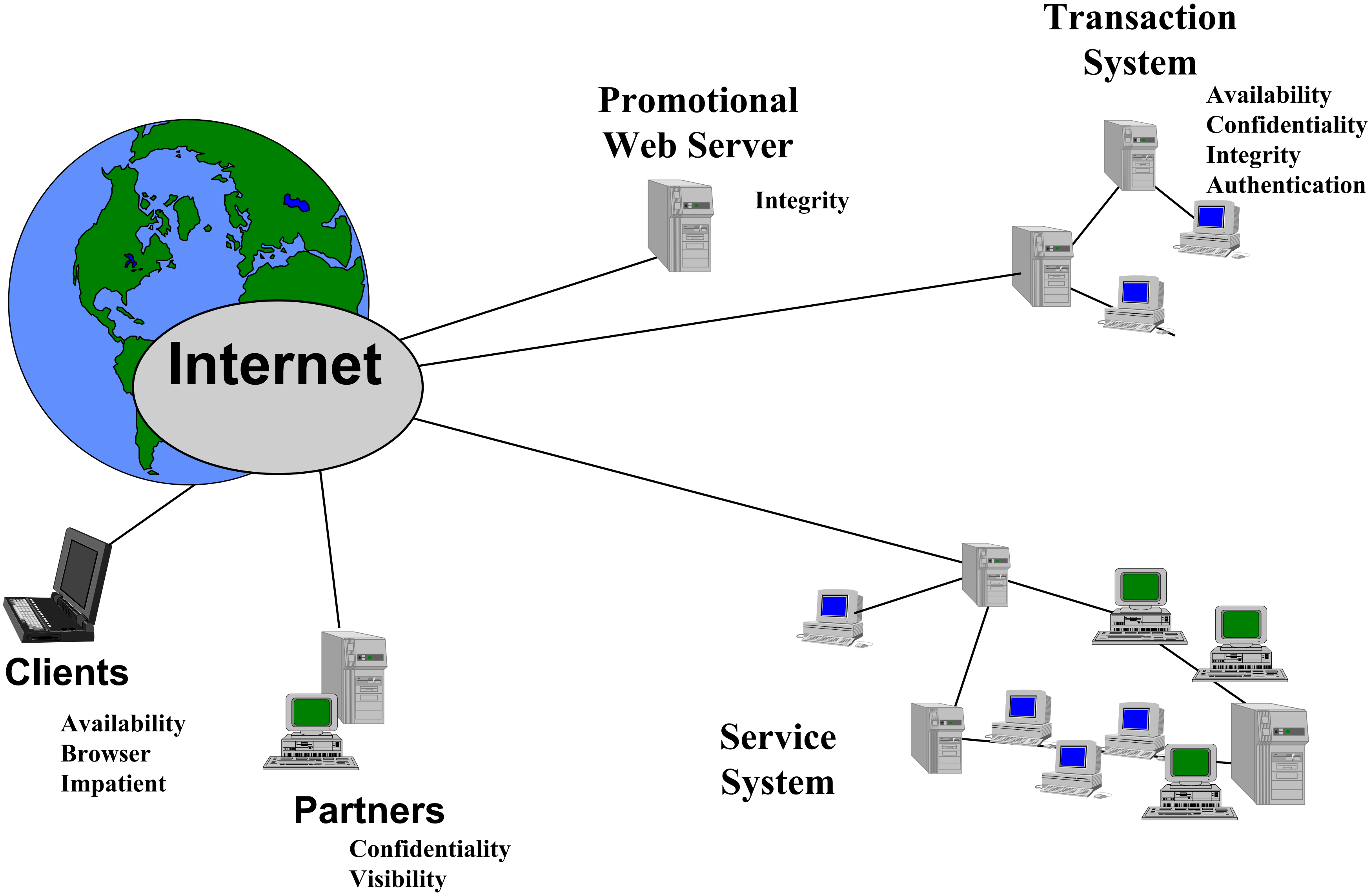
Non-Repudiation

- The ability to prove that information was sent or received by a user or system.
- Other words are: “Signature approval”, “Certified”, ...

Typical Evolving Network



Business/Security Requirements



Internet

Promotional Web Server

Integrity

Transaction System

Availability
Confidentiality
Integrity
Authentication

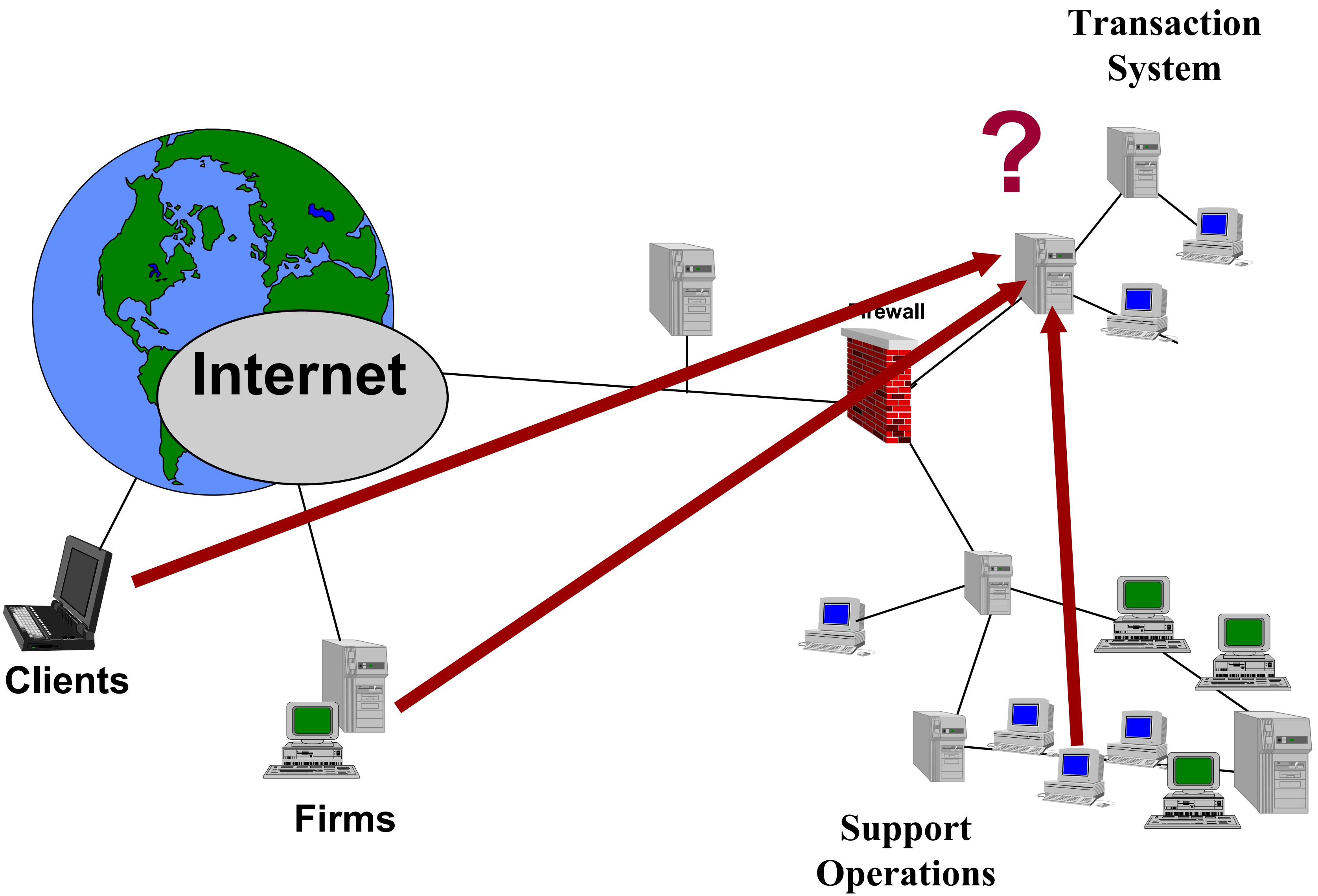
Clients

Availability
Browser
Impatient

Partners

Confidentiality
Visibility

Service System

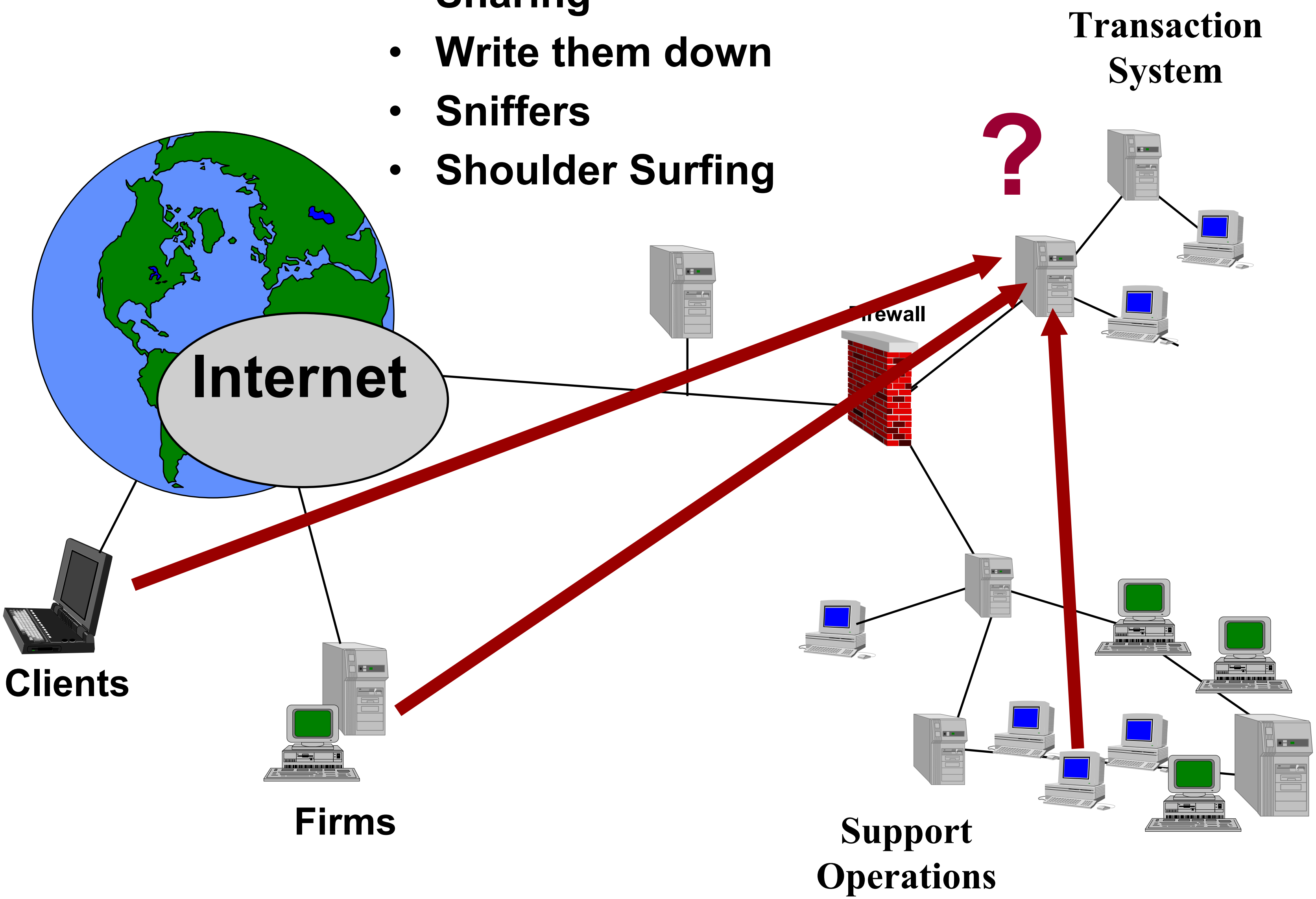

Transaction System
?
Internet
Firewall
Clients
Firms
Support Operations

Configuration

- Defaults
- Passwords
- Backups
- Open Ports
- Filtering
- Logging
- CGI
- Unicode
- ISAPI
- IIS RDS
- NETBIOSv
- Null Sessions
- LM Hash
- RPC Services
- Sendmail
- Bind
- R Commands
- Remote Print LPD
- Sadmind and mountd
- Default SNMP Strings

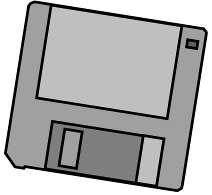
From: http://www.sans.org/top20.htm, April 8, 2002

- Weak Passwords
- Sharing
- Write them down
- Sniffers
- Shoulder Surfing



Authentication Solutions

- Software



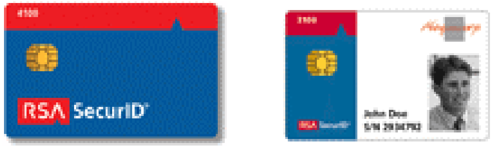
PGP
Netscape
Explorer
Many others

- and

- PCMCIA Card

Spyrus
Fortezza

- Smart Cards

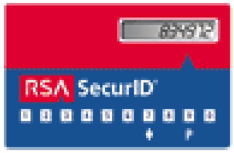


- Computer Chip

DataKey
Rainbow iKey

- ID Tokens

RSA
Secure Computing

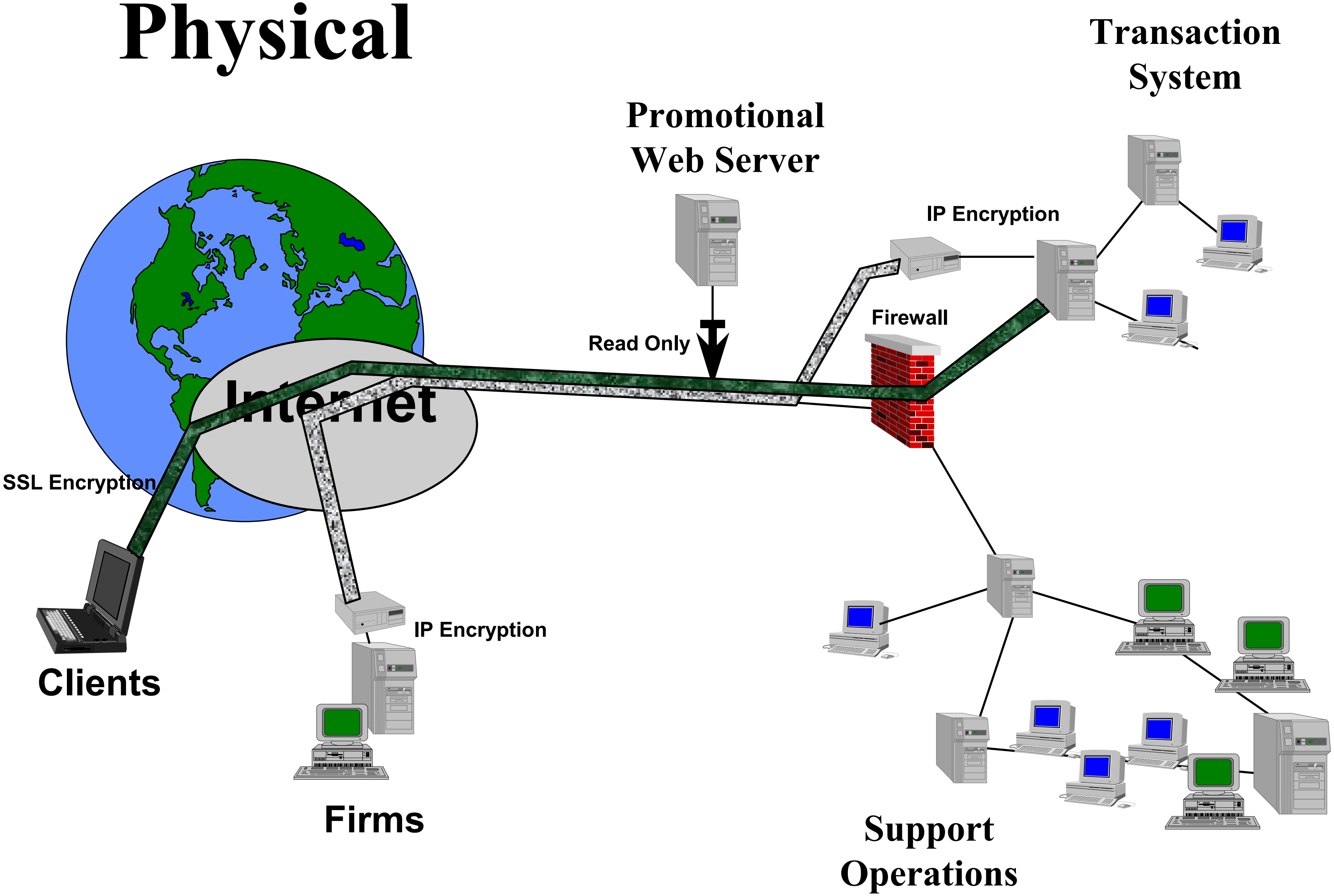


Biometrics

Authenticam™
Panasonic

http://www.identix.com/itsecurity/products/index.html

Physical

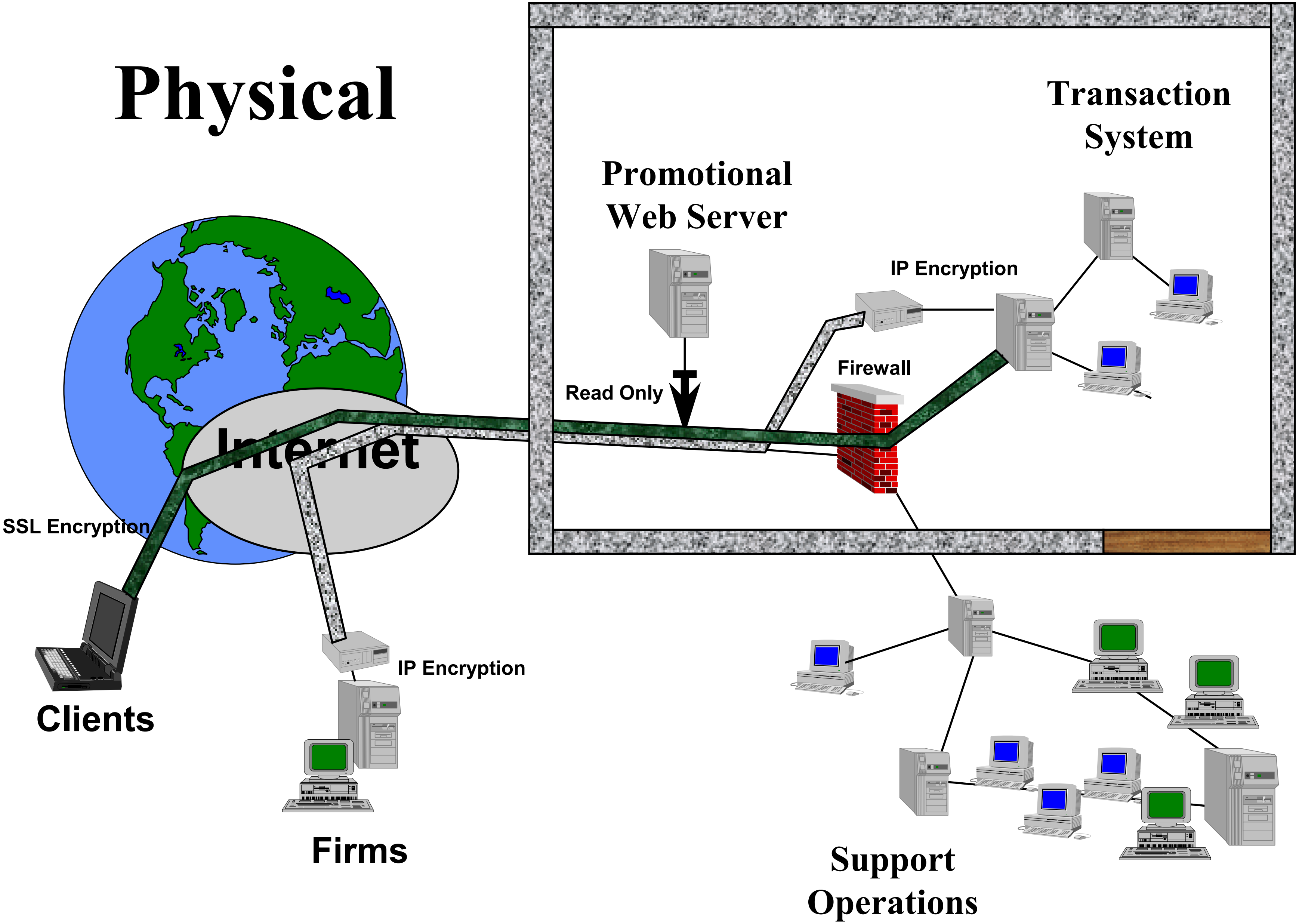

Transaction System
Promotional Web Server
IP Encryption
Firewall
Read Only
Internet
SSL Encryption
IP Encryption
Clients
Firms
Support Operations

Procedures

- Initial entry
  - Last name and first name
  - Change password on first login
- Departures
  - Delete account prior to departure, except…..

- Audit Results
  - 60+% continued “first name” past anniversary date
- Personal Experience
  - Forwarding email continued for months

Physical


Promotional
Web Server
Transaction
System
IP Encryption
Firewall
Read Only
Internet
SSL Encryption
IP Encryption
Clients
Firms
Support
Operations

Who is the Insider Threat?

- Senior Management
- IT Systems Managers
- Users
- Configuration
- Awareness
- Recovery

Litchko & Associates, Inc.

Secure Business-based Solutions^{tm}

Countering the Insider Threat

The right way and the wrong way.

September 25, 2003

Jim Litchko
301-661-3984
jim@litchko.com